

**KELLEY DRYE & WARREN LLP**

A LIMITED LIABILITY PARTNERSHIP

**WASHINGTON HARBOUR, SUITE 400**

**3050 K STREET, NW**

**WASHINGTON, D.C. 20007-5108**

(202) 342-8400

NEW YORK, NY

CHICAGO, IL

STAMFORD, CT

PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES

MUMBAI, INDIA

FACSIMILE

(202) 342-8451

www.kelleydrye.com

DIRECT LINE: (202) 342-8640

EMAIL: dcrock@kelleydrye.com

February 21, 2008

**VIA ECFS**

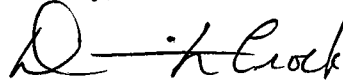
Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12th Street S.W.  
Washington, D.C. 20554

Re: Annual Customer Proprietary Network Information Compliance  
Certification; EB Docket No. 06-36

Dear Ms. Dortch:

Please find the attached Annual Customer Proprietary Network Information ("CPNI") Compliance Certification for Reach Services, USA, Inc. Please feel free to call me if you have any questions regarding this filing.

Sincerely,



Devin L. Crock

Attachment

**Annual Customer Proprietary Network Information Certification**  
**Pursuant to 47 C.F.R. § 64.2009(e)**  
**EB Docket No. 06-36**  
**February 21, 2008**

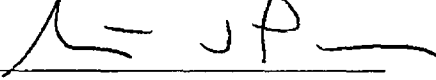
Reach Services USA, Inc.  
Form 499 Filer ID: 822078  
Name of Signatory: Steve Parillo  
Title of Signatory: Vice President Finance

I, Steve Parillo, certify that I am an officer of Reach Service USA, Inc. ("REACH"), and acting as an agent of REACH, that I have personal knowledge that REACH has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how REACH's procedures ensure the company is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the Commission's rules.

REACH has not taken any actions (instituted proceedings or filed petitions at either state commissions, courts, or at the FCC) against data brokers in the past year. REACH has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (*e.g.*, through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps the company has taken to protect CPNI include updating its CPNI practices and procedures and conducting new training designed to ensure compliance with the FCC's modified CPNI rules.

REACH has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

  
\_\_\_\_\_  
Steve Parillo  
Vice President Finance  
REACH Services USA, Inc.

Date: February 21 2008

## **Customer Proprietary Network Information Certification Attachment A**

REACH has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures, which have been updated so that they are adequate to ensure compliance with the Commission's CPNI rules, as modified by the Commission in 2007.

### **Safeguarding against pretexting**

- REACH takes reasonable measures to protect CPNI and believes that these measures are sufficient to prevent unauthorized access to CPNI.

### **Training and discipline**

- REACH has trained its personnel in the appropriate use of CPNI. All employees with access to CPNI are required to review REACH's CPNI manual. REACH employees are required to review REACH's CPNI practices and procedures set forth in REACH's CPNI manual.
- REACH has disciplinary process in place for violations of REACH's practices and procedures which would encompass any misuse of CPNI.

### **REACH's use of CPNI**

- REACH does not share, disclose, or otherwise provide CPNI to any third parties.
- REACH may use CPNI for the following purposes:
  - To initiate, render, maintain, repair, bill and collect for services;
  - To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
  - To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
  - To market additional services to customers that are within the same categories of service to which the customer already subscribes;
- REACH does not disclose or permit access to CPNI to track customers that call competing service providers.
- REACH discloses and permits access to CPNI where required by law (*e.g.*, under a lawfully issued subpoena).

### **Customer approval and informed consent**

- REACH does not use CPNI for any purpose that would require customer approval to do so. For example, REACH does not use CPNI for any marketing purposes and does not share, disclose, or otherwise provide CPNI to any third party. If this policy changes in the future,

REACH will implement practices and procedures to ensure compliance with the Commission's CPNI regulations.

**Additional safeguards**

- REACH has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules.
- REACH designates one or more officers, as an agent or agents of the company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC rule 64.2009(e).
- REACH does not provide or disclose CPNI over the telephone or online, and REACH does not have any retail locations at which it might disclose CPNI to customers in person.
- REACH notifies customers immediately of any account changes.
- REACH may negotiate alternative authentication procedures for services that REACH provides to business customers that have both a dedicated account representative and a contract that specifically addresses REACH's protection of CPNI.
- In the event of a breach of CPNI, REACH will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs REACH to delay notification, or REACH and the investigatory party agree to an earlier notification. REACH will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.